UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,995	12/01/2003	Nancy Cam Winget	72255/00010	3154

23380 7590 04/10/2009
TUCKER ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
04/10/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@tuckerellis.com
christopher.luoma@tuckerellis.com

Office Action Summary	**Application No.** 10/724,995	**Applicant(s)** WINGET ET AL.	
	Examiner JEFFREY D. POPHAM	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-10,15-21,24,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-10,15-21,24,26 and 27* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Remarks

Claims 1, 2, 5-10, 15-21, 24, 26, and 27 are pending.

Response to Arguments

1. Applicant's arguments filed 1/30/2009 have been fully considered but they are not persuasive.

Applicant argues that “Dogan does not teach or suggest receiving a shared secret via a first secure tunnel established between a peer and a server using asymmetric encryption.” Paragraph 23 of Dogan, for example, explicitly states that “the terminal generates the master secret in a random fashion, and provides the master secret to the base station using public key cryptography. In one embodiment, the master secret is established during registration.” This communication that is protected using public key cryptography (e.g. registration connection that encrypts the master secret using public key cryptography) corresponds to the first secure tunnel of claim 1. Public key cryptography is described as being asymmetric in paragraph 4 of the instant application, for example, and such is well known in the art. One can see from the above that the master secret may be exchanged using public key cryptography, such an exchange equating to a first secure tunnel that uses asymmetric cryptography.

Applicant argues that Dogan does not teach or suggest “cryptographically binding a subsequent secure tunnel with conversations inside the tunnel". Applicant continues by stating that "Cryptographic binding of the tunnel with the conversation inside the tunnel helps prevent man-in-the-middle attacks which enable an adversary to take control of information between a peer and a server." Dogan describes that the subsequent secure tunnels are cryptographically protected via the connection secret that is generated from the master secret. Therefore, since only the originating device (e.g. user terminal) and terminating device (e.g. base station) can generate this connection secret, and all communication in this connection is secured with the connection secret, no adversary can take control of information between the entities. The limitation states "cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel" (claim 1). This appears to solely mean that the entities communicate inside the tunnel in a cryptographic manner. The cryptographic binding is made by securing all communication within connection with the connection secret used as a symmetric encryption key. Since the entities of Dogan communicate inside the subsequent new secure tunnel by using the connection secret (paragraph 35, for example), this limitation is clearly found within Dogan.

Claim Objections

2. Claims 1 and 24 are objected to because of the following informalities:

Each of claims 1 and 24 refers to the subsequent, new secure tunnel in multiple manners. Claim 1, for example, refers to "the subsequent secure tunnel" in the "authenticating" limitation before any such subsequent secure tunnel has been set forth in the claim. Claim 24 refers to "the subsequent new tunnel" in the final limitation before any such subsequent new tunnel has been set forth in the claim. It appears as though each of these instances is supposed to be referring to "the subsequent, new secure tunnel" and has been construed as such.

Furthermore, claim 24 states, as the final limitation, that “the wireless device is configured to derive keying material that binds the subsequent new tunnel with all conversations inside the subsequent new tunnel.” Since the wireless device has already been described as being configured to mutually derive a tunnel key for the subsequent, new secure tunnel, this limitation is unclear as to what the keying material is and how it may differ from the tunnel key. It appears as though they are meant to be the same, such that the tunnel key is equivalent to the keying material, and has been construed as such.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 5, 6, 9, 10, 15-21, 24, 26, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dogan (U.S. Patent Application Publication 2004/0268126) in view of Kuehr-McLaren (U.S. Patent 6,978,298) and Funk (PAUL FUNK, Simon Blake Wilson; “draft-ietf-eap-ttls-02.txt: EAP

Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; 30 Nov. 2002, pp. 1-40).

Regarding Claim 1,

Dogan discloses a method of authenticating communication between a first and a second party, the method comprising:

Establishing a first secure tunnel between the peer and the server using asymmetric encryption if a shared secret does not exist between the two (Paragraphs 22-23);

Receiving the shared secret via the first secure tunnel between the peer and the sever responsive to the shared secret not previously existing and establishing the first secure tunnel (Paragraphs 22-23);

Tearing down the first tunnel (Figure 2A; and Paragraphs 7 and 22-24; although "tearing down" is not explicitly stated, it is clear that the registration connection is decoupled from the connections that are later opened, and that the registration connection/tunnel is terminated once the parameters discussed in paragraphs 22-23 are distributed);

Establishing a subsequent, new secure tunnel between the peer and the server using symmetric encryption and the shared secret after tearing down the first tunnel and after the peer has received the shared secret (Paragraphs 24-26);

Mutually deriving a tunnel key for the subsequent new secure tunnel using symmetric cryptography based on the shared secret responsive to establishing the subsequent, new secure tunnel (Paragraphs 24-26);

Authenticating a relationship between the peer and the server within the subsequent secure tunnel upon mutually deriving the tunnel key for the subsequent new secure tunnel (Paragraphs 24-26; this relationship is authenticated by the fact that both entities, and only those entities, can generate the connection secret); and

Cryptographically binding the subsequent new secure tunnel with conversations inside the subsequent new secure tunnel (Abstract; Figure 2A, step 208; and Paragraphs 7, 25, and 35);

But does not explicitly disclose determining whether a shared secret exists between a peer and a server.

Kuehr-McLaren, however, discloses determining whether a shared secret exists between a peer and a server (Column 6, line 29 to Column 7, line 25; and Column 11, lines 12-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management system of Kuehr-McLaren into the secret/key generation system of Dogan in order to allow the system to cache session information for a particular amount of time and dynamically modify and/or update the amount of time based upon the needs of the system and its users, thereby allowing for optimized performance while maintaining a high level of security.

Funk, however, discloses authenticating both the peer and the server to each other by means other than the mere fact that both entities can generate the correct key or secret (Pages 8-10, sections 4.1-4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the extensible authentication system of Funk into the secret/key generation system of Dogan as modified by Kuehr-McLaren in order to provide a number of authentication mechanisms that can be used to authenticate entities in the system, while protecting the authentication information such that it cannot be accessed by any entities that cannot derive the connection secret/tunnel key, thereby providing additional security in the system.

Regarding Claim 17,

Claim 17 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user (Paragraphs 22-25); and Funk discloses protecting the termination of the authenticated conversation by use of a tunnel encryption and authentication to protect against a denial of service by an unauthorized user (Pages 9-15, sections 4.3-6.4).

Regarding Claim 5,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses that the shared secret is a protected access credential (Paragraphs 22-25).

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 5, in addition, Dogan discloses that the protected access credential includes a protected access credential key (Paragraphs 22-25).

Regarding Claim 9,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 6, in addition, Funk discloses that the protected access credential includes a protected access credential opaque element (Pages 3-4, section 1; and Pages 10-13, sections 5-6.2).

Regarding Claim 10,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 6, in addition, Funk discloses that the protected access credential includes a protected access credential information element (Pages 11-13, sections 6-6.2).

Regarding Claim 15,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Funk discloses that the step of authenticating is performed using EAP-GTC (Pages 21-22, section 10.2.1).

Regarding Claim 16,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Funk discloses that the step of authenticating is performed using Microsoft MS-CHAP v2 (Pages 23-24, section 10.2.4).

Regarding Claim 18,

Dogan as modified by Kuehr-McLaren and Funk discloses the system of claim 17, in addition, Funk discloses that the communication link is a wireless network (Pages 4-5, section 2).

Regarding Claim 19,

Dogan as modified by Kuehr-McLaren and Funk discloses the system of claim 17, in addition, Funk discloses that the communication link is a wired network (Pages 4-5, section 2).

Regarding Claim 21,

Dogan as modified by Kuehr-McLaren and Funk discloses the system of claim 18, in addition, Funk discloses t hat the wireless network is an 802.11 wireless network (Pages 4-5, section 2).

Regarding Claim 24,

Dogan discloses a wireless device comprising:

A wireless network adapter for sending and receiving wireless signals with a server (Paragraphs 33-34);

Wherein the wireless device is configured to receive a shared secret from the server if no shared secret exists with the server, by establishing a first secure tunnel with the server using asymmetric encryption, receiving the shared secret via the first secure tunnel from the server, and tearing down the first secure tunnel after receiving the shared secret (Paragraphs 7, 22-24, 34, and 51);

Wherein the wireless device is configured to establish a subsequent, new secure tunnel between the wireless device and the server after the first tunnel has been torn down and if the shared secret exists by using the shared secret to mutually derive a tunnel key using symmetric cryptography based on the shared secret (Paragraphs 24-26);

Wherein the wireless device is configured to mutually authenticate with the server employing the subsequent new secure tunnel (Paragraphs 24-26); and

Wherein the wireless device is configured to derive keying material that binds the subsequent, new secure tunnel with all conversations inside the subsequent, new secure tunnel (Abstract; Figure 2A, step 208; and Paragraphs 7, 25, and 35);

But does not explicitly disclose determining whether a shared secret exists between a peer and a server.

Kuehr-McLaren, however, discloses determining whether a shared secret exists between a peer and a server, and receiving the shared secret upon determining that a shared secret does not exist with the server (Column 6, line 29 to Column 7, line 25; and Column 11, lines 12-32). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the session management system of Kuehr-McLaren into the secret/key generation system of Dogan in order to allow the system to cache session information for a particular amount of time and dynamically modify and/or update the amount of time based upon the needs of the system and its users, thereby allowing for optimized performance while maintaining a high level of security.

Funk, however, discloses authenticating both the peer and the server to each other by means other than the mere fact that both entities can generate the correct key or secret (Pages 8-10, sections 4.1-4.3; Pages 11-13, sections 6-6.2; and Page 20, section 10). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the extensible authentication system of Funk into the secret/key generation system of Dogan as modified by Kuehr-McLaren in order to provide a number of authentication mechanisms that can be used to authenticate entities in the system, while protecting the authentication information such that it cannot be accessed by any entities that cannot derive the connection secret/tunnel key, thereby providing additional security in the system.

Regarding Claim 26,

Dogan as modified by Kuehr-McLaren and Funk discloses the device of claim 24, in addition, Funk discloses that the wireless device is further configured to establish a session key seed for deriving a master session key used for mutually authenticating the wireless device employing the subsequent secure tunnel (Pages 11-16, sections 6-7).

Regarding Claim 27,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses establishing a plurality of subsequent new secure tunnels between the peer and server using the shared secret (Paragraphs 7, 22-26, and claim 10).

4. Claims 5-10 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dogan in view of Kuehr-McLaren and Funk, further in view of Downnard (Downnard, Ian, "Public-key cryptography extensions into Kerberos", IEEE December 2002/January 2003, pp. 30-34).

Regarding Claim 5,

Dogan as modified by Kuehr-McLaren and Funk discloses the method of claim 1, in addition, Dogan discloses that the shared secret is a protected access credential (Paragraphs 22-25); but does not explicitly disclose certain aspects of such a protected access credential.

Downnard, however, discloses that the shared secret is a protected access credential (Pages 30 and 32, Kerberos and PKINIT sections). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the public-key-extended Kerberos system of Downnard into the EAP-TTLS system of Dogan as modified by Kuehr-McLaren and Funk in order to ensure authentication of entities wishing to communicate as well as a trusted party that distributes shared secret information, while improving security and scalability through use of public keys for initial authentication.

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 5, in addition, Downnard discloses that the protected access credential includes a protected access credential key (Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 7,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 6, in addition, Funk discloses that the protected access credential key is a strong entropy key (Page 16, section 7); and Downnard discloses that the protected access credential key is a strong entropy key (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 8,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 7, in addition, Downnard discloses that the entropy key is a 32-octet key (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 9,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 6, in addition, Downnard discloses that the protected access credential includes a protected access credential opaque element (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Regarding Claim 10,

Dogan as modified by Kuehr-McLaren, Funk, and Downnard discloses the method of claim 6, in addition, Downnard discloses that the protected access credential includes a protected access credential information element (Table 1; and Pages 30 and 32, Kerberos and PKINIT sections).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2437

/Jeffrey D Popham/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437